

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA §
Plaintiff, §
§
v. § NO:6:24-CV-00200
§
\$116,764.56 IN UNITED STATES §
CURRENCY §
Defendant. §

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been so employed since September 2001. My current position is the Resident Agent in Charge (RAIC) of the USSS Tyler Resident Office. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law enforcement officer of the United States, in that I am empowered by law to conduct

investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

- a. \$74,684.89 in JP Morgan Chase (JPMC) Bank account 559393320 (Target Account 1);
- b. \$21,478.95 in JPMC Bank account 558182880 (Target Account 2);
- c. \$5,000.13 in JPMC account 5017020753 (Target Account 3);
- d. \$15,600.59 in JPMC account 5017587702 (Target Account 4);

that totals \$116,764.56, which were cumulatively directed into Check No. 4557192445 and was seized on or about March 5, 2024, in Tyler, Texas pursuant to a seizure warrant.

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term “spoofed” refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S.

based victims, to include victims located in the Eastern District of Texas. Scammers then fooled victims into “investing” in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims’ money.

5. This type of scam is often identified as “pig butchering” (derived from the Chinese phrase, which is used to describe this scheme) and involves scammers spending significant time getting to know, targeting and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH or USDC deposit address, and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim’s account balance, which entices the victim to continue making investments, which typically end with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to “significant profits” gained on the account or other reasons such as freezing the account due to “taxes owed” or “suspicious behavior.” Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve a large portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or

1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a “financial transaction” with proceeds from “specified unlawful activity” (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of “money laundering” as defined by 18 U.S.C. § 1956 is to disguise the illicit nature of funds by introducing it into legitimate commerce and finance thereby making them “clean.” This financial process is most commonly conducted using three steps referred to as “placement,” “layering,” and “integration.” Typically, the “placement” phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. “Layering” takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the “integration” phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property

constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 or a conspiracy to commit such offense (18 U.S.C. § 1349). Wire fraud is a SUA.

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or 1349 is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

- a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;
- b. It is not a defense that those funds have been removed and replaced by other funds; and
- c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the “guilty” property had been kept.

FACTS SUPPORTING FORFEITURE

14. The United States is investigating a pig butchering scheme involving a fraudulent cryptocurrency investment scheme that utilizes spoofed domains. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from pig butchering victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of the pig butchering victims. The Elights Trading Inc. bank account was provided to victims located within the Eastern District of Texas as a means in which they would pay their “taxes and/or fees” concerning their “earnings” as part of this scheme.

16. Investigators interviewed multiple victims who sent funds to the Citibank held in the name of Elights Trading. In summary, these victims reported to have been tricked into believing they were investing in cryptocurrency, when in fact they were provided with links or information leading them to use spoofed domains or applications of legitimate cryptocurrency exchanges. One of these victims was identified as T.G.

17. Investigators interviewed victim T.G. regarding the \$230,000 transaction remitted to the ELIGHTS TRADING Account. T.G. met a friend on Facebook in or about May 2023, but has never met this individual face to face. T.G.’s new female friend portrayed herself as being very wealthy and T.G. inquired how he could invest money to earn a large and safe return. T.G.’s friend provided a link to Telegram where he was led to believe he was working with employees of OKEX, a cryptocurrency exchange. T.G. received instructions via Telegram regarding investments, including the information for the ELIGHTS TRADING account. T.G. stated he believed he was purchasing options in cryptocurrency and not specific cryptocurrency coins such as Bitcoin. T.G. has invested approximately \$850,000 in total by sending to other bank accounts he received from the

OKEX Telegram communications. T.G. stated he has only requested small withdrawals from his investment and has received only a few thousand dollars and has not made any large withdrawal requests.

18. T.G. informed USSS investigators that during this scheme, he was provided the JPMC Bank account in the name of SUNSHINES TRADING, account number ending in 2181. A review of JPMC Bank records pertaining to this account reflect T.G. sent \$80,000 to this account on September 20, 2023.

19. USSS investigators conducted an investigation of SUNSHINES TRADING which included obtaining bank records via grand jury subpoena. USSS investigators reviewed these bank records and identified additional victims of the fraud scheme, to include B.H.

Victim B.H.

20. USSS investigators interviewed victim B.H. regarding the \$80,000.00 transaction he sent to the JPMC account in the name of SUNSHINES TRADING, account number ending in 8678. B.H. was also victimized by this cryptocurrency investment scheme. It all began by meeting a person on Facebook who used the name Mona Johnson Chen. B.H. stated Chen introduced him to the OKX platform. B.H. suffered a loss of approximately \$352,000.00 as a result of this scheme to the following entities: SUNSHINES TRADING, ROYAL CHRONOS LIMITED, and BLUEWAVE TRADE LIMITED. B.H. recently attempted to withdraw his funds from OKX but was informed he would need to pay \$19,000 in taxes and/or fees prior to receiving his funds.

**INVESTIGATION OF BLUEWAVE TRADE LIMITED LEADS TO
IDENTIFICATION OF TARGET ACCOUNT 1**

21. USSS investigators initiated an investigation of BLUEWAVE TRADE LIMITED (BTL) which held bank accounts at JPMC Bank. USSS investigators learned from JPMC employees that BTL operated a bank account that was recently closed by JPMC. JPMC employees advised USSS investigators that the signor on the BTL account was identified as Yuxuan Chen, who was also identified as the signor on a JPMC account in the name of Eagleeye Group Limited (EGL).

22. USSS investigators obtained JPMC bank records for the accounts held in the name of EGL (TARGET ACCOUNT 1) and 2880 (TARGET ACCOUNT 2).

23. TARGET ACCOUNT 1 records indicate the account was opened on or about October 17, 2023, and Yuxuan Chen is listed as the signor and beneficiary in these documents. The records indicate that on or about September 13, 2023, Yuxuan Chen established EGL in California as a C-Corporation. The records also indicate the address for EGL is 811 West 7th Street, Suite 1200, Los Angeles, California 90017.¹ Investigators were unable to locate an Internet business presence for EGL.

24. Analysis of the records related to TARGET ACCOUNT 1 indicate the account's activity from October 18, 2023, to November 15, 2023, included several deposits via wire transfers and other payments, such as Zelle transactions, totaling approximately \$1,461,463.00. The transaction activity was similar to other accounts identified in this investigation which received proceeds of the fraudulent cryptocurrency

¹ Earlier in this investigation, USSS investigators identified the address utilized by EGL was also used by other shell companies in this investigation, including Royal Chronos Limited, whose account was seized under seizure warrant number 6:24-MJ-5.

investment scheme. There were also two JPMC bank transfers from TARGET ACCOUNT 2 into TARGET ACCOUNT 1 totaling \$60,000. These funds were derived from wire transactions from victims of this fraud scheme.

25. The most significant withdrawals from TARGET ACCOUNT 1 include ten wire transfers to a Wells Fargo account held in the name of Magic Location Trading² totaling approximately \$1,318,785.00.

26. The following wire deposits were made into TARGET ACCOUNT 1 and are a sampling of the total deposits into TARGET ACCOUNT 1:

Date	Amount	Victim
10/26/2023	\$10,000	G.C.
10/26/2023	\$150,000	D-W.C.
10/26/2023	\$100,000	S.D.
10/27/2023	\$100,000	S.D.
10/27/2023	\$10,500	M.S.S.
10/27/2023	\$8,544	G.P.M
10/30/2023	\$5,000	G.M.S.
10/30/2023	\$5,000	R.B.K.
10/30/2023	\$9,000	K.F.P.
10/30/2023	\$25,000	E.J.A.
10/30/2023	\$10,000	P.L.P.
10/31/2023	\$6,000	A.T.D.
10/31/2023	\$5,000	M.R.A.N.
10/31/2023	\$50,000	J.K.P.
10/31/2023	\$100,000	W.F.P.
11/1/2023	\$20,000	A.A.
11/1/2023	\$26,000	D.L.
11/1/2023	\$3,000	Q.P.
11/2/2023	\$5,000	M.B.C.
11/3/2023	\$25,000	THE G.S.R.T.
11/6/2023	\$86,000	S.F.TRUST
11/6/2023	\$25,000	J.D.B.
11/7/2023	\$55,000	B.I.LLC
11/7/2023	\$24,500	J.D.B. 2ND

² Earlier in this investigation, USSS investigators identified shell company Magic Location Trading with accounts at several banks, including JPMC. The Magic Location Trading JPMC account was previously seized as part of this investigation under seizure warrant number 6:23-MJ-259.

Date	Amount	Victim
		DEPOSIT
11/8/2023	\$20,000	K.G.N.
11/8/2023	\$350,000	U.D.L.
11/8/2023	\$8,000	J.M.F.B
11/9/2023	\$11,863.48	A.E.F.P.
11/9/2023	\$20,000	D.K.W.
11/9/2023	\$20,178	T.T.P.D.
11/9/2023	\$6,000	A.S.
11/9/2023	\$10,000	S.C.
11/10/2023	\$5,000	G.R.L. TRUST
11/10/2023	\$10,000	A.L.L.
11/13/2023	\$10,000	A.L.
11/13/2023	\$56,000	J.D.
		A.E.F.P. 2ND DEPOSIT
11/14/2023	\$8,917.43	
11/14/2023	\$36,959.72	P.M.H.
11/14/2023	\$15,000	D.R.B.
11/15/2023	\$10,001.03	T.P.

INTERVIEWS OF ADDITIONAL VICTIMS THAT SENT FUNDS TO TARGET ACCOUNT 1

27. In addition to victim B.H. who sent funds as a result of this fraud scheme to an account (Bluewave Trade Limited) also owned by Yuxuan Chen, investigators interviewed additional victims who were identified as having sent funds to TARGET ACCOUNT 1 (owned by Chen) as part of the cryptocurrency investment fraud scheme.

Victim P.L.P.

28. USSS investigators identified and interviewed victim P.L.P. regarding the \$10,000 he sent to TARGET ACCOUNT 1. P.L.P. acknowledged he was a victim of an investment fraud scheme and has not been able to recover any of his funds. P.L.P. explained he met an unknown individual on a dating app and then moved their conversation to WhatsApp. P.L.P. stated the individual introduced him to a platform that operated in a similar fashion as an Amazon store. P.L.P. mentioned the platform had

various items to sell, where he would be responsible for maintaining the inventory by purchasing goods to sell in the online store. P.L.P.’s initial investments were for products in the store that sold at a very rapid pace, enticing him to send funds to purchase more “inventory.” P.L.P. stated his requests to have the inventory purchased with the “profit” were denied. P.L.P. believed the online websites to essentially be “straw stores” where there was evidently nothing that was ever sold/purchased. P.L.P. never physically witnessed any sort of products that was selling.

29. P.L.P. stated the online shop’s addresses were <https://familyshopco.com/wap/#/home> and <https://familyshopw.com/www/#/login>.

30. P.L.P. provided USSS investigators with transaction details of the funds he sent to various bank accounts as part of this scheme. The transactions began in August 24, 2023, and ended on November 24, 2023, totaling approximately \$136,447.00. One of the receiving accounts included a PNC bank account in the name of Quick Book Trade, which was known to USSS investigators in this investigation.

Victim J.D.

31. USSS investigators interviewed J.D. regarding the \$56,000 transaction he sent to TARGET ACCOUNT 1 on November 13, 2023. J.D. acknowledged he wired the funds during his involvement in a cryptocurrency investment scheme. J.D. explained that in or about September 2023 he received a “wrong number call” from someone using the name Haru LNU, who called from 929-270-1013. Haru LNU introduced J.D. to a platform identified as m.perioex.com wherein he could invest in cryptocurrency and earn a very large return. J.D. stated that the platform required him to purchase a membership that would allow him to pay a reduced tax rate on his earnings. J.D. stated the

membership fee was \$128,000. J.D. believed he was purchasing a membership by completing the \$56,000 transaction to EGL and \$72,000 to an additional account also under USSS investigation.

32. J.D. explained that after he completed the transfers, he logged into his account at m.peroex.com and communicated with the customer service feature on the website. J.D. stated the customer service representative informed him that the accounts sent to him were fraudulent and that he needed to respond to his bank to issue a wire recall. J.D. has not been able to recover any portion of his funds.

33. Based on my experience conducting fraud investigations, fraudsters closely monitor the available bank accounts they use to accept fraud proceeds. Once the fraudsters learn that the bank accounts have been closed and/or restricted by bank and/or law enforcement personnel, the fraudsters will alert the victim to recall their funds and redirect the victims to deposit the funds in a different account.

Victim P.H.

34. USSS investigators interviewed victim P.H. regarding the \$36,959.72 transaction he sent to TARGET ACCOUNT 1 on November 14, 2023. P.H. acknowledged he was the victim of a cryptocurrency investment scheme that was initiated by an errant text message from someone using the name Emma Baker. P.H. was first contacted by Baker on or about May 4, 2023, and continued to communicate with Baker via various WhatsApp numbers to include: 310.844.2170, 743.888.3985, 213.619.2995 and +49-152-1645-6971.

35. P.H. explained the conversation with Baker turned to investing in cryptocurrency, specifically with the platforms coin-ex.plug.com/p/m (mobile use); coin-

ex.plug.com/p/pc (computer); m.morgansox.cc#/user; pc.morgansox.cc/#/. P.H. stated Baker introduced him to these platforms. P.H.'s initial investments with these platforms were small.

36. P.H. stated the proceeds of his initial investments were returned to him, which enticed him to invest more funds. P.H. was also provided JPMC account 522196990 in the name of Jiao Jiao Liu, address 1000 W 8th Street, Suite 828, Los Angeles, California.³ P.H. was only provided this account to send funds to, but P.H. did not send any payment to this account.

37. P.H. stated the transaction to the JPMC EGL account was made to pay "taxes." P.H. explained he was not able to make additional withdrawals from any of his accounts at the above listed platforms, as he was informed he needed to pay taxes on his earnings before he could make a withdrawal. P.H. communicated with a customer service representative on the platforms morgansox and coin-ex.plug. P.H. stated that after the transaction was sent, he was informed the amount of \$36,959.72 was not the correct amount and additional funds were needed. P.H. was not able to withdraw any of his funds. P.H. believed his account balance reflected an amount of approximately \$189,000.

38. Shortly after P.H. sent the transaction to the EGL JPMC account, he stated the customer service representative of coin-ex.plug platform instructed him to respond to his bank to recall the transaction. P.H.'s efforts to recall the funds were unsuccessful.

³ Earlier in this investigation, USSS investigators identified shell company Stonewater Trading with a bank account at JPMC wherein Jiao Jiao Liu was identified as the owner of the account and utilized the same address. The Stonewater Trading JPMC account was previously seized as part of this investigation under seizure warrant number 6:23-MJ-270.

INTERNET CRIME COMPLAINT CENTER REPORTS REGARDING TARGET ACCOUNT 1

39. USSS investigators queried the Internet Crime Complaint Center (IC3) regarding TARGET ACCOUNT 1. The reports identified four additional victims of this fraud scheme who reportedly sent TARGET ACCOUNT 1 a combined amount of approximately \$124,179.03. Some of these victims also sent additional funds to other shell companies identified in this investigation.

INVESTIGATION IDENTIFIES TARGET ACCOUNT 2 AS RECEIVING VICTIMS' FUNDS

40. USSS investigators identified TARGET ACCOUNT 2 held in the name of Yuxuan Chen. USSS investigators reviewed the bank records for TARGET ACCOUNT 2 and discovered that this account was also utilized to receive funds from victims of this investment fraud scheme.

41. Bank records reveal that TARGET ACCOUNT 2 was opened on or about October 11, 2023, and the signor on the account is Yuxuan Chen, the same signor as on TARGET ACCOUNT 1. The address utilized for this account is 900 S. Figueroa Street, Apartment 808, Los Angeles, California 90015.

42. Analysis of the bank records for TARGET ACCOUNT 2 indicate the account received deposits totaling approximately \$120,789. The transaction activity was similar to other accounts identified in this investigation which received proceeds of the fraudulent cryptocurrency investment scheme.

43. The withdrawal activity includes transactions to TARGET ACCOUNT 1, specifically \$60,000.00 in debits related to daily living expenses and travel to Las Vegas, Nevada.

44. The following wire deposits are examples of the deposits that were made into TARGET ACCOUNT 2:

Date	Amount	Victim
10/16/2023	\$46,968	A.G.J.
10/30/2023	\$4,000	M.R.
11/1/2023	\$5,000	E.G.P.
11/1/2023	\$2,000	P.H.
11/3/2023	\$2,000	G.C.
11/3/2023	\$7,608	G.D.J.
11/3/2023	\$2,000	G.J.J.
11/6/2023	\$1,000	L.A.H.
11/6/2023	\$5,000	T.N.
11/6/2023	\$10,000	J.S.
11/7/2023	\$3,000	G.C. 2ND WIRE
11/7/2023	\$5,213	L.H.
11/8/2023	\$15,000	M.K.C.
11/9/2023	\$7,000	M.S.S.
11/15/2023	\$5,000	F.W.F.

INTERVIEW OF VICTIMS WHO SENT FUNDS TO TARGET ACCOUNT 2

Victim E.G.P.

45. USSS investigators identified and interviewed victim E.G.P. regarding the \$5,000.00 transaction he sent to TARGET ACCOUNT 2. E.G.P. stated that in October 2023, he met “Anna” on Facebook after he went through a divorce. E.G.P. stated their conversation quickly turned to Anna’s investment into what E.G.P. identified as a “crypto.com-defi wallet.” E.G.P. mentioned that Anna demonstrated how the platform was earning her a large return on her investments and encouraged E.G.P. to invest. E.G.P. stated he was able to establish an account on this platform. E.G.P. advised USSS investigators that Anna enticed him further by making it appear as if she funded E.G.P.’s account with \$48,000 as a method to demonstrate the rapid growth and earnings the platform earns.

46. E.G.P. made multiple small investments on the platform to include \$3,185 via Crypto.com, \$1,000 via CashApp, and \$5,000 to TARGET ACCOUNT 2. E.G.P. was soon needed to withdraw funds from his account on the platform to pay for bills and living expenses. E.G.P. recently attempted to withdraw \$15,000 from his account but was informed he would need to deposit \$100,000 before he could make a withdrawal. E.G.P. felt uneasy about the platform from the beginning, but since he has been unable to withdraw funds from the account, he feels that he has lost his funds as a result of this scheme.

Victim T.N.

47. USSS investigators identified and interviewed victim T.N. regarding the \$5,000.00 transaction he sent to TARGET ACCOUNT 2. T.N. advised that in or about August 2023, he received a wrong number call from a female and they continued to communicate despite not knowing each other. T.N. stated their communications turned to earning a large return by investing in gold futures. The unknown person introduced T.N. to a platform noted as Phemexcs, where T.N. was made to believe he was investing in gold futures. T.N. sent multiple transactions as part of this scheme that totaled approximately \$60,000.00. T.N. invested in this platform because the unknown person he was communicating with informed him he could earn profits of 13%. T.N. was unable to withdraw his funds from Phemexcs and was informed that he needed to pay a fee/tax equal to 10% of his earnings.

Victim F.W.F.

48. USSS investigators identified and interviewed victim F.W.F. regarding the \$5,000.00 transaction he sent to TARGET ACCOUNT 2. F.W.F. encountered an Asian

female using the name “Anna Nie” on Facebook. F.W.F. stated Nie was boasting about her investments in ETH using a platform identified as Bifrost. Nie directed F.W.F. to the Google store where he could download Bifrost. F.W.F. was able to download the Bifrost app from the Google store and made several investments to fund his account totaling \$77,000.00.

49. F.W.F.’s initial investment of \$5,000 that he sent to TARGET ACCOUNT 2 was reflected in the Bifrost app and earned \$130 per day. F.W.F. was informed by Nie that he could earn a greater return by investing more funds. After sending additional funds, F.W.F.’s account reflected that he was earning \$17,000 to \$20,000 per day. But F.W.F. has not been able to withdraw any of the funds.

50. F.W.F. also sent information to USSS investigators that he was provided as part of this scheme when sending wire transactions. The information appeared to be “tips” on how to avoid scrutiny from financial institutions. The information provided by F.W.F. states:

“in the bank wire transfer, please choose to expedite or fast remittance, so that out of the bank backstage will not have to audit, reducing the risk of the funds are intercepted; prohibit the transfer of remarks: investment money, loans, money. 3, prohibit the transfer of remarks: investment money, loans, zero money. Recharge, financial payment, BTC USDT digital currency forex lottery PC MT5 MT4, do not make a note of tax payment or loan, borrowing and other words!”

51. This information was provided to F.W.F. via email from a sender using email address abbyyu027@gmail.com.

FUNDS ARE SENT FROM TARGET ACCOUNT 2 TO TARGET ACCOUNT 3

52. USSS investigators reviewed the JPMC bank records associated with TARGET ACCOUNT 3. The records indicate the account is also held in the name of

Yuxuan Chen with address 811 West 7th Street, Suite 1200, Los Angeles, California 90017. This address is also used by other individuals previously identified in this investigation. These records indicate that TARGET ACCOUNT 3 received a deposit of \$5,000 from TARGET ACCOUNT 2 on or about November 13, 2023.

TARGET ACCOUNT 4 RECEIVED FRAUD PROCEEDS

53. USSS investigators obtained JPMC bank records for TARGET ACCOUNT 4 via grand jury subpoena. These records indicate TARGET ACCOUNT 4 (JPMC account ending in 7702) is held in the name of Eagle Eye Group Limited and Yuxuan Chen is also the signor on this account. According to the records, TARGET ACCOUNT 4 was opened by Chen on or about October 17, 2023.

54. USSS investigators reviewed the transactions for TARGET ACCOUNT 4 which included a \$65,600 deposit from JPMC account ending in 7169. JPMC account 7169 is in the name of Bluewave Trade Limited and is also in the name of Yuxuan Chen. The JPMC account ending in 7169 received direct victim funds from previously identified victim B.H. who sent \$100,00 to the JPMC account ending in 7169 on or about October 13, 2023. The only other transaction in TARGET ACCOUNT 4 included a withdrawal of \$50,000.00 to TARGET ACCOUNT 1. The remaining balance of approximately \$15,600.59 in TARGET ACCOUNT 4 was provided to the USSS as part of this seizure by JPMC.

CONCLUSION

55. I submit that this affidavit supports probable cause to forfeit all funds, monies, and other things of value up to \$116,764.56 seized from JPMC Bank accounts:

- a. \$74,684.89 in JP Morgan Chase (JPMC) Bank account 559393320 (Target Account 1);
- b. \$21,478.95 in JPMC Bank account 558182880 (Target Account 2);
- c. \$5,000.13 in JPMC account 5017020753 (Target Account 3);
- d. \$15,600.59 in JPMC account 5017587702 (Target Account 4);

56. Based on my experience and the information herein, I have probable cause to believe that the seized \$116,764.56 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

57. I also have probable cause to believe that the seized \$116,764.56 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

58. As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

 Digitally signed by bschley
Date: 2024.06.03 11:42:45
-05'00'

Brad Schley, Special Agent
U.S. Secret Service